EXHIBIT B

PLR 4-3(b) – The Parties' Construction of Disputed Terms & Phrases

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
1.	aspect 683.2 861.58 900.155 912.8	Feature, element, property or state.	An aspect of an environment is a persistent element or property of that environment that can be used to distinguish it from other environments.
2.	authentication 193.15	Identifying (e.g., a person, device, organization, document, file, etc.). Includes uniquely identifying or identifying as a member of a group.	To establish that the following asserted characteristics of something (e.g., a person, device, organization, document, file, etc.) are genuine: its identity, its data integrity, (i.e., it has not been altered) and its origin integrity (i.e., its source and time of origination).
3.	budget 193.1	Information specifying a limitation on usage.	(1) A unique type of "method" that specifies a decrementable numerical limitation on future **Use** (e.g., copying) of digital information and how such **Use** will be paid for, if at all. (2) A "method" is a collection of basic instructions, and information related to basic instructions, that provides context, data, requirements, and/or relationships for use in performing, and/or preparing to perform, basic instructions in relation to the operation of one or more electronic appliances.
4.	clearinghouse 193.19	A provider of financial and/or administrative services for a number of entities; or an entity responsible for the collection, maintenance, and/or distribution of materials, information, licenses, etc.	(1) A computer system that provides intermediate storing and forwarding services for both content and audit information, and which two or more parties trust to provide its services independently because it is operated under constraint of **VDE** security. (2) "Audit information" means all information created, stored, or reported in connection with an "auditing" process. "Auditing"

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			means tracking, metering and reporting the usage of particular information or a particular appliance.
5.	compares 900.155	Normal English: examines for the purpose of noting similarities and differences.	A processor operation that evaluates two quantities and sets one of three flag conditions as a result of the comparison – greater than, less than, or equal to.
6.	component assembly 912.8, 912.35	Components are code and/or data elements that are independently deliverable. A Component Assembly is two or more components associated together. Component Assemblies are utilized to perform operating system and/or applications tasks.	(1) A cohesive **Executable** component created by a channel which binds or links together two or more independently deliverable *Load Modules* (see below), and associated data. (2) A **Component Assembly** is assembled, and executes, only within a **VDE** *Secure Processing Environment* (see below). (3) A **Component Assembly** is assembled dynamically in response to, and to service, a particular content-related activity (e.g., a particular **Use** request). (4) Each **VDE Component Assembly** is assigned and dedicated to a particular activity, particular user(s), and particular protected information. (5) Each **Component Assembly** is independently assembled, loadable and deliverable vis-à-vis other **Component Assemblies.** (6) The dynamic assembly of a **Component Assembly** is directed by a "blueprint" *Record* (see below) **Containing** control information for this particular activity on this particular information by this particular user(s). (7) **Component Assemblies** are extensible and can be configured and reconfigured (modified) by all users, and combined by all users with other **Component Assemblies,**

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			subject only to other users' "senior" **Controls**. For the purposes of the construction of "Component Assembly," a "*Load Module*" is defined as follows: An **Executable**, modular unit of machine code (which may include data) suitable for loading into memory for execution by a processor. A load module is encrypted (when not within a secure processing unit) and has an **Identifier** that a calling process must provide to be able to use the load module. A load module is combinable with other load modules, and associated data, to form **Executable Component Assemblies**. A load module can execute only in a **VDE Protected Processing Environment**. Library routines are not load modules and dynamic link libraries are not load modules. For the purposes of the construction of "Component Assembly," a "*Secure Processing Environment*" is defined as follows: A Secure Processing Environment is uniquely identifiable, self-contained, non-circumventable, and trusted by all other **VDE** nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the patent application as being protected, and to guarantee that such information will be accessed and **Used** only as expressly authorized by the associated **VDE Controls**, and to guarantee that all requested reporting of and payments for protected information use will be made. A Secure Processing

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			Environment is formed by, and requires, a Secure Processing Unit having a hardware **Tamper Resistant Barrier** encapsulating a processor and internal **Secure** memory. The **Tamper Resistant Barrier** prevents all unauthorized interference, removal, observation, and other **Use** of the information and processes within it. For the purposes of the construction of "Component Assembly," a "*Record*" is defined as follows: A data structure that is a collection of fields (elements), each with its own name and type. Unlike an array, whose elements are accessed using an index, the elements of a record are accessed by name. A record can be accessed as a collective unit of elements, or the elements can be accessed individually.
7.	contain 683.2 912.8, 912.35	Normal English: to have within or to hold. In the context of an element contained within a data structure (e.g., a secure container), the contained element may be either directly within the container or the container may hold a reference indicating where the element may be found.	Physically (directly) storing within, as opposed to addressing (i.e., referring to something by the explicitly identified location where it is stored, without directly storing it).
8.	control (n.) 193.1, 193.11, 193.15, 193.19 683.2 891.1	Information and/or programming controlling operations on or use of resources (e.g., content) including (a) permitted, required or prevented operations, (b) the nature or extent of such operations or (c) the consequences of such operations.	(1) Independent, special-purpose, **Executable**, which can execute only within a *Secure Processing Environment.* (2) Each **VDE Control** is a **Component Assembly** dedicated to a particular activity (e.g., editing, modifying another **Control**, a user-defined action, etc.), particular user(s), and particular protected information, and whose satisfactory execution is necessary to *Allowing* (see below) that activity.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			(3) Each separate information *Access* (see below) or **Use** is independently **Controlled** by independent **VDE Control(s)**. (4) Each **VDE Control** is assembled within a *Secure Processing Environment* from independently deliverable modular components (e.g., *Load Modules* or other **Controls**), dynamically in response to an information *Access* or **Use** Request. (5) The dynamic assembly of a **Control** is directed by a "blueprint" *Record* (put in place by one or more **VDE** users) **Containing** control information identifying the exact modular code components to be assembled and executed to govern (i.e., **Control**) this particular activity on this particular information by this particular user(s). (6) Each **Control** is independently assembled, loaded and delivered vis-à-vis other **Controls**. (7) Control information and **Controls** are extensible and can be configured and modified by all users, and combined by all users with any other **VDE** control information or **Controls** (including that provided by other users), subject only to "senior" user **Controls**. (8) Users can assign control information (including alternative control information) and **Controls** to an arbitrarily fine, user-defined portion of the protected information, such as a single paragraph of a document, as opposed to being limited to file-based controls. (9) **VDE Controls** reliably limit **Use** of the protected information to only authorized activities and amounts.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			For the purposes of the construction of "Control," a "*Secure Processing Environment*" is defined as set forth in item #6, above. For the purposes of the construction of "Control," "*Allowing*" is defined as follows: Actively permitting an action that otherwise cannot be taken (i.e., is prohibited) by any user, process, or device. In **VDE**, an action is allowed only through execution (within a *Secure Processing Environment*) of the **VDE Control(s)** assigned to the particular action request, and satisfaction of all requirements imposed by such execution. For the purposes of the construction of "Control," "*Access*" is defined as follows: To satisfactorily perform the steps necessary to obtain something so that it can be **Used** in some manner (e.g., for information: copied, printed, decrypted, encrypted, saved, modified, observed, or moved, etc.). In **VDE**, access to protected information is achieved only through execution (within a *Secure Processing Environment*) of the **VDE Control(s)** assigned to the particular "access" request, satisfaction of all requirements imposed by such execution, and the **Controlled** opening of the **Secure Container Containing** the information. For the purposes of the construction of "Control," "*Load Module*" and "*Record*" are defined as set forth in item #6, above.
9.	controlling, control (v.)	Normal English: to exercise authoritative or dominating influence over; direct.	(1) Reliably defining and enforcing the conditions and requirements under which an action that otherwise

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
	193.1 861.58		cannot be taken, will be *Allowed*, and the manner in which it may occur. Absent verified satisfaction of those conditions and requirements, the action cannot be taken by any user, process or device. (2) In **VDE**, an action is **Controlled** through execution of the applicable **VDE Control(s)** within a **VDE** *Secure Processing Environment*. (3) More specifically, in **VDE**, **Controlling** is effected by use of **VDE Controls**, **VDE Secure Containers**, and **VDE** foundation (including **VDE** *Secure Processing Environment*, "object registration," and other mechanisms for allegedly individually ensuring that specific **Controls** are enforced vis-à-vis specific objects (and their content at an arbitrary granular level) and specific "users"). For the purposes of the construction of "Control (v.)" et al, "*Allowed*" is defined as set forth in item #8, above, and "*Secure Processing Environment*" is defined as set forth in item #6, above.
10.	copy, copied, copying 193.1, 193.11, 193.15, 193.19	Reproduce, reproduced, reproducing. The reproduction must be usable, may incorporate all of the original item or only some of it, and may involve some changes to the item as long as the essential nature of the content remains unchanged.	(1) To reproduce all of a *Digital File* or other complete physical block of data from one location on a storage medium to another location on the same or different storage medium, leaving the original block of data unchanged, such that two distinct and independent objects exist. (2) Although the layout of the data values in physical storage may differ from the original, the resulting "copy" is logically indistinguishable from the original. (3) The resulting "copy" may or may not be encrypted, ephemeral, usable, or accessible.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			For the purposes of the construction of "Copy," et al, a *"Digital File"* is defined as: A named, static unit of storage allocated by a "file system" and **Containing** digital information. A digital file enables any application using the "file system" to randomly access its contents and to distinguish it by name from every other such unit. A copy of a digital file is a separate digital file. A "file system" is the portion of the operating system that translates requests made by application programs for operations on "files" into low-level tasks that can control storage devices such as disk drives.
11.	derive 900.155	Normal English: obtain, receive or arrive at through a process of reasoning or deduction. In the context of computer operations, the "process of reasoning or deduction" constitutes operations carried out by the computer.	To retrieve from a specified source.
12.	designating 721.1	Normal English: indicating, specifying, pointing out or characterizing.	Designating something for a particular **Use** means specifying it for and restricting it to that **Use**.
13.	device class 721.1	A group of devices which share at least one attribute.	The generic name for a group of device types. For example, all display stations belong to the same device class. A device class is different from a device type. A device type is composed of all devices that share a common model number or family (e.g. IBM 4331 printers).
14.	digital signature, digitally signing 721.1	digital signature: A digital value, verifiable with a key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.). Digitally signing is the process of creating a digital signature.	digital signature: A computationally unforgeable string of characters (e.g., bits) generated by a cryptographic operation on a block of data using some secret. The string can be generated only by an entity that knows the secret, and hence provides evidence that the

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			entity must have generated it. digitally signing: (1) Creating a **Digital Signature** using a secret *Key* (see below). (2) In symmetric key cryptography, a "secret key" is a *Key* that is known only to the sender and recipient. In asymmetric key cryptography, a "secret key" is the private *Key* of a public/private key pair, in which the two keys are related uniquely by a predetermined mathematical relationship such that it is computationally infeasible to determine one from the other. For the purposes of the construction of "Digital Signature" and "Digital Signing," a "*Key*" is defined as: A bit sequence used and needed by a cryptographic algorithm to encrypt a block of plain text or to decrypt a block of cipher text. A key is different from a key seed or other information from which the actual encryption and/or decryption key is constructed, **Derived**, or otherwise identified. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric or "public key" cryptography, two related keys are used; a block of text encrypted by one of the two keys (e.g., the "public key") can be decrypted only by the corresponding key (e.g., the "private key").
15.	executable programming, executable 721.34 912.8, 912.35	A computer program that can be run, directly or through interpretation.	executable: A cohesive series of machine code instructions in a format that can be loaded into memory and run (executed) by a connected processor.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			executable programming: A cohesive series of machine code instructions, comprising a computer program, in a format that can be loaded into memory and run (executed) by a connected processor. A "computer program" is a complete series of definitions and instructions that when executed on a computer will perform a required or requested task.
16.	host processing environment 900.155	This term is explicitly defined in the claim and therefore needs no additional definition. It consists of those elements listed in the claim. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: a Protected Processing Environment incorporating software-based security.	(1) A processing environment within a **VDE** node which is not a *Secure Processing Environment*. (2) A "host processing environment" may either be "secure" or "not secure." (3) A "secure host processing environment" is a self-contained **Protected Processing Environment**, formed by loaded, **Executable** programming executing on a general purpose CPU (not a Secure Processing Unit) running in protected (privileged) mode. (4) A "non-secure host processing environment" is formed by loaded, **Executable** programming executing on a general purpose CPU (not a Secure Processing Unit) running in user mode. For the purposes of the construction of "host processing environment," a "*Secure Processing Environment*" is defined as set forth in item #6, above.
17.	identifier 193.15 912.8	Information used to identify something or someone (e.g., a password). In this definition, "identify" means to establish the identity of or to ascertain the origin, nature, or	Any text string used as a label naming an individual instance of what it *Identifies*. For the purpose of the construction of "Identifier," "Identify" is defined as: To establish as being a particular

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
		definitive characteristics of; includes identifying as an individual or as a member of a group.	instance of a person or thing.
18.	protected processing environment 683.2 721.34	An environment in which processing and/or data is at least in part protected from tampering. The level of protection can vary, depending on the threat. In this definition, "environment" means capabilities available to a program running on a computer or other device or to the user of a computer or other device. Depending on the context, the environment may be in a single device (e.g., a personal computer) or may be spread among multiple devices (e.g., a network).	(1) A uniquely identifiable, self-contained computing base trusted by all **VDE** nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the February, 1995, patent application as being protected, and to guarantee that such information will be *Accessed* and **Used** only as expressly authorized by **VDE Controls**. (2) At most **VDE** nodes, the **Protected Processing Environment** is a *Secure Processing Environment* which is formed by, and requires, a hardware **Tamper Resistant Barrier** encapsulating a special-purpose Secure Processing Unit having a processor and internal secure memory. "Encapsulated" means hidden within an object so that it is not directly accessible but rather is accessible only through the object's restrictive interface. (3) The **Tamper Resistant Barrier** prevents all unauthorized (intentional or accidental) interference, removal, observation, and use of the information and processes within it, by all parties (including all users of the device in which the **Protected Processing Environment** resides), except as expressly authorized by **VDE Controls**. (4) A **Protected Processing Environment** is under **Control** of **Controls** and control information provided by one or more parties, rather than being under **Control** of the appliance's users or programs. (5) Where a **VDE** node is an

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			established financial **Clearinghouse**, or other such facility employing physical facility and user-identity **Authentication** security procedures trusted by all **VDE** nodes, and the **VDE** node does not *Access* or **Use** **VDE**-protected information, or assign **VDE** control information, then the **Protected Processing Environment** at that **VDE** node may instead be formed by a general-purpose CPU that executes all **VDE** "security" processes in protected (privileged) mode. (6) A **Protected Processing Environment** requires more than just verifying the integrity of **Digitally Signed Executable** programming prior to execution of the programming; or concealment of the program, associated data, and execution of the program code; or use of a password as its protection mechanism. For the purposes of the construction of "Protected Processing Environment," a "*Secure Processing Environment*" is defined as set forth in item #6, above, and "*Access*" is defined as set forth in item #8, above.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
19.	secure, securely 193.1, 193.11, 193.15 683.2 721.34 861.58 891.1 912.8, 912.35	One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control. Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined. Access control means that access to information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose.	(1) A state in which all users of a system are guaranteed that all information, processes, and devices within the system, shall have their availability, secrecy, integrity, authenticity and nonrepudiation maintained against all of the identified threats thereto. (2) "Availability" means the property that information is accessible and usable upon demand by authorized persons, at least to the extent that no user may delete the information without authorization. (3) "Secrecy," also referred to as confidentiality, means the property that information (including computer processes) is not made available or disclosed to unauthorized persons or processes. (4) "Integrity" means the property that information has not been altered either intentionally or accidentally. (5) "Authenticity" means the property that the characteristics asserted about a person, device, program, information, or process are genuine and timely, particularly as to identity, data integrity, and origin integrity. (6) "Nonrepudiation" means the property that a sender of information cannot deny its origination and that a recipient of information cannot deny its receipt.
20.	secure container 683.2 861.58 912.35	A container that is Secure. In this definition, "container" means a digital file containing linked and/or embedded items.	(1) A **VDE Secure Container** is a self-contained, self-protecting data structure which (a) encapsulates information of arbitrary size, type, format, and organization, including other, nested, containers, (b) cryptographically protects that information from all unauthorized *Access* and Use, (c) provides encrypted storage management

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			functions for that information, such as hiding the physical storage location(s) of its protected contents, (d) permits the association of itself or its contents with **Controls** and control information governing (**Controlling**) *Access* to and **Use** thereof, and (e) prevents such **Use** or *Access* (as opposed to merely preventing decryption) until it is "opened." (2) A **Secure Container** can be opened only as expressly *Allowed* by the associated **VDE Control(s)**, only within a *Secure Processing Environment*, and only through decryption of its encrypted header. (3) A **Secure Container** is not directly accessible to any non-**VDE** or user calling process. All such calls are intercepted by **VDE**. (4) The creator of a **Secure Container** can assign (or allow others to assign) control information to any arbitrary portion of a **Secure Container**'s contents, or to an empty **Secure Container** (to govern (**Control**) the later addition of contents to the container, and *Access* to or **Use** of those contents). (5) A container is not a **Secure Container** merely because its contents are encrypted and signed. A **Secure Container** is itself **Secure**. (6) All **VDE**-protected information (including protected content, information about content usage, content-control information, **Controls**, and *Load Modules*) is encapsulated within a **Secure Container** whenever stored outside a *Secure Processing Environment* or secure database.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			For the purposes of the construction of "Secure Container," "*Secure Processing Environment*" and "*Load Module*" are defined as set forth in item #6, above, and "*Access*" and "*Allow*" are defined as set forth in item #8, above.
21.	tamper resistance 721.1	Making tampering more difficult and/or allowing detection of tampering. In this definition, "tampering" means using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use.	tamper resistance: The ability of a **Tamper Resistant Barrier** to prevent *Access*, observation, and interference with information or processing encapsulated by the barrier. For the purposes of the construction of "Tamper Resistance," "*Tamper/Tampering*" is defined as: Using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use. For the purposes of the construction of "Tamper Resistance," "*Access*" is defined as set forth in item # 6, above.
22.	tamper resistant barrier 721.34	Hardware and/or software that provides Tamper Resistance.	(1) An active device that encapsulates and separates a **Protected Processing Environment** from the rest of the world. (2) It prevents information and processes within the **Protected Processing Environment** from being observed, interfered with, and leaving except under appropriate conditions ensuring security. (3) It also **Controls** external access to the encapsulated **Secure** resources, processes and information. (4) A **Tamper Resistant Barrier** is capable of destroying protected information in response to *Tampering* attempts. For the purposes of the construction

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			of "Tamper Resistant Barrier," "*Tamper/Tampering*" is defined as set forth in item #21, above.
23.	use 193.19 683.2 721.1 861.58 891.1 912.8, 912.35	Normal English: to put into service or apply for a purpose, to employ.	(1) To use information is to perform some action on it or with it (e.g., copying, printing, decrypting, encrypting, saving, modifying, observing, or moving, etc.). (2) In **VDE**, information **Use** is *Allowed* only through execution of the applicable **VDE Control(s)** and satisfaction of all requirements imposed by such execution. For the purposes of the construction of "Use," "*Allowed*" is defined as set forth in item #8 above.
24.	virtual distribution environment 900.155 Also as set forth in each "claim as a whole" by Microsoft.	This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements. The term "virtual distribution environment" should not be read into claims that do not actually recite it. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: secure, distributed electronic transaction management and rights protection system for controlling the distribution and/or other usage of electronically provided and/or stored information.	VDE/Virtual Distribution Environment: (1) Data Security and Commerce World: InterTrust's February 13, 1995, patent application described as its "invention" a **Virtual Distribution Environment** ("VDE invention") for securing, administering, and auditing all security and commerce digital information within its multi-node world (community). **VDE** guarantees to all **VDE** "participants" identified in the patent application that it will limit all *Access* to and **Use** (i.e., interaction) of such information to authorized activities and amounts, will ensure any requested reporting of and payment for such **Use**, and will maintain the availability, secrecy, integrity, non-repudiation and authenticity of all such information present at any of its nodes (including protected content, information about content usage, and content **Controls**.).

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			VDE is **Secure** against at least the threats identified in the Feburary 1995, patent application to this availability (no user may delete the information without authorization), secrecy (neither available nor disclosed to unauthorized persons or processes), integrity (neither intentional nor accidental alteration), non-repudiation (neither the receiver can disavow the receipt of a message nor can the sender disavow the origination of that message) and authenticity (asserted characteristics are genuine). **VDE** further provides and requires the components and capabilities described below. Anything less than or different than this is not **VDE** or the described "invention." (2) Secure Processing Environment: At each node where **VDE**-protected information is *Accessed*, **Used**, or assigned control information, **VDE** requires a *Secure Processing Environment* (as set forth in item #6). (3) VDE Controls: **VDE Allows** *Access* to or **Use** of protected information and processes only through execution of (and satisfaction of the requirements imposed by) **VDE Control(s)**. (4) VDE Secure Container: See construction of **Secure Container**. (5) Non-Circumventable: **VDE** is non-circumventable (sequestered). It intercepts all attempts by any and all users, processes, and devices, to *Access* or **Use**, such as observing, interfering with, or removing) protected information, and prevents all such attempts other than as

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			allowed by execution of (and satisfaction of all requirements imposed by) associated **VDE Controls** within *Secure Processing Environment(s)*. (6) Peer to Peer: **VDE** is peer-to-peer. Each **VDE** node has the innate ability to perform any role identified in the patent application (e.g., end user, content packager, distributor, **Clearinghouse**, etc.), and can protect information flowing in any direction between any nodes. **VDE** is not client-server. It does not pre-designate and restrict one or more nodes to act solely as a "server" (a provider of information (e.g., authored content, control information, etc.) to other nodes) or "client" (a requestor of such information). All types of protected-content transactions can proceed without requiring interaction with any server. (7) Comprehensive Range of Functions: **VDE** comprehensively governs (**Controls**) all security and commerce activities identified in the patent application, including (a) metering, budgeting, monitoring, reporting, and auditing information usage, (b) billing and paying for information usage, and (c) negotiating, signing and enforcing contracts that establish users' rights to *Access* or **Use** information. (8) User-Configurable: The specific protections governing (**Controlling**) specific **VDE**-protected information are specified, modified, and negotiated by **VDE**'s users. For example, **VDE** enables a consumer to place limits on the nature of content that may be *Accessed* at her

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			node (e.g., no R-rated material) or the amount of money she can spend on viewing certain content, both subject only to other users' senior **Controls**. (9) General Purpose; Universal: **VDE** is universal as opposed to being limited to or requiring any particular type of appliance, information, or commerce model. It is a single, unified standard and environment within which an unlimited range of electronic rights protection, data security, electronic currency, and banking applications can run. (10) Flexible: **VDE** is more flexible than traditional information security and commerce systems. For example, **VDE** allows consumers to pay for only the user-defined portion of information that the user actually uses, and to pay only in proportion to any quantifiable **VDE** event (e.g., for only the number of paragraphs displayed from a book), and allows editing the content in **VDE** containers while maintaining its security. For the purposes of the construction of "VDE," a "*Secure Processing Environment*" is defined as set forth in item #6, above. For the purposes of the construction of "VDE," "*Access*" is defined as set forth in item #8, above.
25.	193.1: "a budget specifying the number of copies which can be made of said digital file"	Normal English, incorporating the separately defined terms: a Budget stating the number of copies that can be made of the digital file referred to earlier in the claim.	A **Budget** explicitly stating the total number of copies (whether or not decrypted, long-lived, or accessible) that (since creation of the **Budget**) are authorized to be made of the *Digital File* by any and all users, devices, and processes. No process,

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			user, or device is able to make another copy of the *Digital File* once this number of copies has been made. For the purposes of the construction of this phrase, "*Digital File*" is defined as set forth in item #6, above.
26.	193.1: "controlling the copies made of said digital file"	The nature of this operation is further defined in later claim elements. In context, the copy control determines the conditions under which a digital file may be Copied and the copied file stored on a second device.	**Controlling Uses** of and *Accesses* to all copies of the *Digital File*, by all users, processes, and devices, by executing each of the recited "at least one" **Copy Control(s)** within **VDE** *Secure Processing Environment(s)*. Each **Control** governs **(Controls)** only one action, which action may or may not differ among the different "at least one" **Controls**. All **Uses** and *Accesses* are prohibited and incapable of occurring except to the extent *Allowed* by the "at least one" **Copy Control(s)**. For the purposes of the construction of this phrase, a "*Secure Processing Environment*" is defined as set forth in item #6, above, and "*Access*" and "*Allowed*" are defined as set forth in item #8, above.
27.	721.1: "digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance	Normal English, incorporating the separately defined terms: generating a Digital Signature for the second load module, the Digital Signature Designating that the second load module is for use by a second Device Class. This element further requires that the second Device Class have a different Tamper Resistance or security level than the first Device Class.	(1) **Digitally Signing** a different ("second") *Load Module* by using a different ("second") **Digital Signature** as the signature *Key*, which signing indicates to any and all devices in the second **Device Class** that the signor authorized and restricted this *Load Module* for **Use** by that device. (2) No **VDE** device can perform any execution of any *Load Module* without such authorization. The method ensures that the *Load Module* cannot execute in a particular **Device Class** and ensures

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
	and security level different from the at least one of tamper resistance and security level of the first device class"		that no device in that **Device Class** has the *Key(s)* necessary to verify the **Digital Signature**. (3) All devices in the first **Device Class** have the same persistent (not just occasional) and identified level of **Tamper Resistance** and the same persistent and identified level of security. All devices in the second **Device Class** have the same persistent and identified level of **Tamper Resistance** and same persistent and identified level of security. (4) The identified level of **Tamper Resistance** or identified level of security (or both) for the first **Device Class**, is greater than or less than the identified level of **Tamper Resistance** or identified level of security for the second **Device Class**. For the purposes of the construction of this phrase, a "*Load Module*" is defined as set forth in item #6, above, and "*Key*" is defined as set forth in item #14, above.
28.	891.1: "securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item"	Normal English, incorporating the separately defined terms: the first entity's Control and the second entity's Control are Securely applied to govern Use of the data item, the act of Securely applying involving use of the resource.	(1) Processing the resource (component part of a first appliance's **Secure** Operating Environment) within the **Secure** Operating Environment's special-purpose Secure Processing Unit (SPU) to execute the first **Control** and second **Control** in combination within the SPU. (2) This execution of these **Controls** governs (**Controls**) all **Use** of the data item by all users, processes, and devices. (3) The processing of the resource and execution of the **Controls** cannot be observed from outside the SPU and is performed only after the

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			integrity of the resource and **Controls** is cryptographically verified. (4) A Secure Processing Unit is a special-purpose unit isolated from the rest of the world in which a hardware **Tamper Resistant Barrier** encapsulates a processor and internal **Secure** memory. (5) The processor cryptographically verifies the integrity of all code loaded from the **Secure** memory prior to execution, executes only the code that the processor has authenticated for its **Use**, and is otherwise **Secure**.
29.	900.155: "derives information from one or more aspects of said host processing environment"	Normal English, incorporating the separately defined terms: Derives (including creates) information based on at least one Aspect of the previously referred to Host Processing Environment	(1) **Deriving** from the **Host Processing Environment** hardware one or more values that uniquely and persistently identify the **Host Processing Environment** and distinguish it from other **Host Processing Environments**. (2) The "one or more aspects of said host processing environment" are persistent elements or properties of the **Host Processing Environment** itself that are capable of being used to distinguish it from other environments, as opposed to, e.g., data or programs stored within the mass storage or main memory, or processes executing within the **Host Processing Environment**.
30.	912.8: "identifying at least one aspect of an execution space required for use and/or execution of the load module"	Normal English, incorporating the separately defined terms: identifying an Aspect (e.g. security level) of an execution space that is needed in order for the load module to execute or otherwise be used.	(1) Defining fully, without reference to any other information, at least one of the persistent elements or properties (**Aspects**) (that are capable of being used to distinguish it from other environments of an execution space) that are required for any **Use**, and/or for any execution, of the *Load Module*. (2) An execution space without all of those required aspects is

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			incapable of making any such execution and/or other **Use** (e.g., **Copying**, displaying, printing) of the *Load Module*. For the purposes of the construction of this phrase, a "*Load Module*" is defined as set forth in item #6, above.